United States Military Academy Faculty Privileged Access Agreement (PAA) and Acknowledgement of Responsibilities

I understand that the United States Military Academy (USMA) has granted me access to the Defense Research and Engineering Network (DREN), and that I have and will maintain the necessary clearances and authorizations for local administrator access to my government furnished equipment (GFE) information system (laptop, desktop, mobile device, etc.)

As a Privileged-level user I will protect my account and my authenticator(s) to the highest level of data or resource it secures.
I will **NOT** share my account and authenticator(s) entrusted for my use.

I am responsible for all actions taken under my account and understand that the exploitation of this account places other systems and assets on the DREN at risk.

I will not attempt to hack the network or connected information systems (ISs), subvert USMA cybersecurity controls or processes, subvert data protection schemes or otherwise expose the DREN to risks that I have no authority to accept. Hacking and security activities in the context of a classroom, assignment, or faculty supervised USMA club activity is exempt from this prohibition when coordinated with, and approved by, the USMA CIO/G6.

I will not gain, access, share, or elevate permissions to data or ISs for which I have no explicit permission from a controlling authority.

I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of system or network services, illegal or improper possession of content or files, or the actual or possible compromise of data, files, access controls, or systems to my chain of command and USMA Cybersecurity Branch.

I will NOT install, modify, or remove any hardware connected to the DREN without permission and approval from my Chain of Command and the USMA CIO/G6 office (e.g., USMA Cybersecurity Branch).

I will not install malicious code of any variety. I will practice due diligence to ensure software/code that I install does not contain known and unpatched vulnerabilities.

I am prohibited from obtaining, installing, copying, pasting, modifying, transferring or using software or other materials in violation of the appropriate owner's/vendor's patent, copyright, trade-secret, or license agreements.

I will not create or elevate access rights of others; share permissions to ISs for which they are not authorized; nor allow others access to ISs or networks using my privileged account.

I am prohibited from accessing, storing, processing, displaying, distributing, transmitting and viewing material that is: pornographic, racist, defamatory, vulgar, hate-crime related, subversive in nature, or involves chain letters, spam, or similarly related criminal offenses such as encouragement of criminal activity, or violation of State, Federal, national, or international law.

I am prohibited from storing, accessing, processing, sharing, removing, or distributing Classified information on the DREN. If I become aware of such information on my GFE IS or other DREN-connected system, I will disconnect the system from the network, while leaving it powered on, and make a report to the USMA Cybersecurity Branch.

I am prohibited from storing, accessing, processing, sharing, removing, or distributing Controlled Unclassified Information (CUI) (e.g., Personally Identifiable Information (PII), Personal Health Information (PHI), For Official Use Only (FOUO)) data in ways that violate USMA policies or other controlling authority policies.

I am prohibited from using, or allowing others to use, Army resources for personal gain such as advertising or solicitation of services or sale of personal property (e.g. eBay) or stock trading.

I am prohibited from employing, using, or distributing personal encryption capabilities (e.g., virtual private network (VPN) software other than USMA-licensed VPN) on DREN-connected systems.

I will contact my chain of command if I am in doubt as to any of my roles, responsibilities, or delegated authorities.

I am subject to loss of elevated access rights on my GFE IS and other forms of disciplinary or punitive action for violating the PAA, authorized Use Policy (AUP), or other controlling documents (e.g., Joint Ethics Regulation, Army Regulations)..

_____ _____

Printed Full Name and Signature / Digital Signature Date